FortiMail

Secure Email Gateway Appliances

(Updated October 2017)

For FortiMail Cloud Managed service see separate the FortiMail Cloud FAQ document.

General FAQs

What is FortiMail?

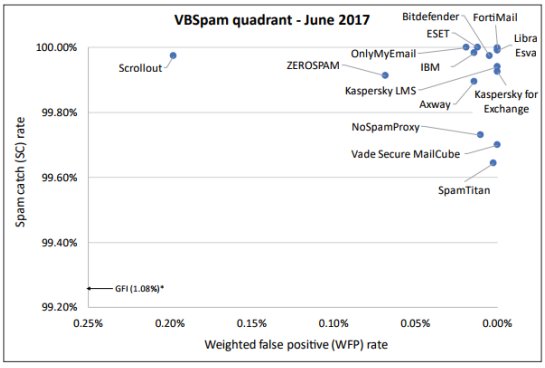
FortiMail is a top-rated secure email gateway that stops volume-based and targeted cyber threats to help secure the dynamic enterprise attack surface, prevents the loss of sensitive data and helps maintain compliance with regulations. High performance physical and virtual appliances deploy on-site or in the public cloud to serve any size organization — from small businesses to carriers, service providers, and large enterprises.

FortiMail can be deployed as a Secure Email Gateway, scanning and securing email before forwarding on to its destination, or as a full Secure Mail Server with users accessing the FortiMail to retrieve their email via the Web, POP3 or IMAP.

Has FortiMail been independently tested?

FortiMail is continually tested as part of VBSPAM certification and regularly receives VMSPAM+ rating. In the most recent test (June 2017) FortiMail was the highest rated vendor with 100% catch rate and 0% false positive.

FortiMail also participates in the ICSA Advanced Threat Defense Testing where the ATP stack including FortiMail, is tested over a 40 day period. ICSA stated that *"With its ATP Solution, Fortinet provides highly effective, comprehensive defense including excellent recognition of previously unknown email-borne threats with few false positives."*



Fortinet ATP Solution

Certified Since December 2016

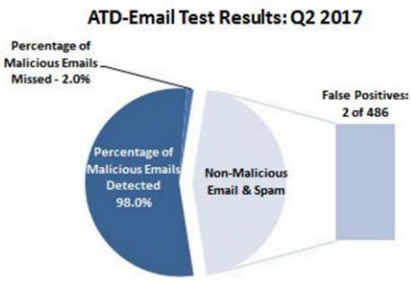


Fig. 2 – 1081 ATD-Email Test Runs

FortiMail is also FIPS 140-2 and Common Criteria EAL2+ (4.2.2) and NDPP (5.2.6) certified

But Gartner placed FortiMail in the niche players quadrant in the latest Magic Quadrant.

This is old news. Gartner chose not to continue the SEG MQ in 2016 so 2015 is the last one but some competitors still advertise this. We disagreed with our positioning then, today we have made significant progress. See the ICSA and VBSpam testing above for real world comparatives.

What are the differences between the various FortiMail models?

In general FortiMail systems provide the same security features. The main difference between devices is email processing performance, hard disk storage capacity redundant power supplies, and RAID storage options. Maximum Values Matrix for each configuration option can be found in Appendix B of the FortiMail Administration Guide.

There are however some functions which are only available on specific models.

Active AV Database(Wildlist)	-	All models
Extended AV Database (ETDB)	-	200E/VM01 and above
Extended+ AV Database (EXDB)	-	1000D/VM04 and above
Central quarantine	-	400E/VM02 and above

How do I size a FortiMail Opportunity?

The key metric to understand when sizing a FortiMail opportunity is what is the peak number of emails per hour that the customer sends and receives? This can then be used to select the correct device based on the performance metrics of the relevant models. Unfortunately this level of information is rarely available so gather whatever metrics are available e.g. number of users, business type, average message size and this can be used to approximate this information.

In general the following rule of thumb can be used to size FortiMail opportunity; however, if you have not sized a FortiMail solution previously, it is recommended that you engage a FortiMail CSE to help with the process.

FortiMail 60D	-	Demo, testing, training and small businesses with fewer than 100 users
FortiMail 200E	-	Small businesses, branch offices and organizations with fewer than 400 users
FortiMail 400E	-	Small-to-midsized organizations with up to 1000 users
FortiMail 1000D	-	Mid-to-large enterprise, education and government departments with up to 3000 users
FortiMail 2000E	-	Large enterprise, education and government departments
FortiMail 3000E	-	Highest performing appliance for the largest University, corporate, ISP and carrier customers
FortiMail 3200E	-	Highest performing appliance for the largest University, corporate, ISP and carrier customers. Supports 10G interfaces.

Feature FAQs

What spam detection features are available with FortiMail?

FortiMail offers both Connection and Content Level spam detection technologies to deliver enterprise-class spam detection capabilities. Complete scanning of the email header and email body including embedded URI's and meta information is performed to ensure the most accurate rates of spam detection.

The FortiMail architecture has been designed to optimize performance and to detect malicious content as soon as possible, with as little resource impact as possible. Detection is performed in order:

Connection based detection methods:

FortiGuard AntiSpam - IP Reputation

3rd Party RBL support

FortiGuard Botnet Tracking Database

Local Dynamic Sender Reputation

Greylisting

Forged IP checking

Session rate limit

Content Header Based Methods:

Recipient verification

SMTP Error Rate Control

Global and User customized Black/White Lists

Deep e-mail header inspection

RFC Compliancy

DHA Protection

Sender Policy Framework (SPF)

Domain-Based Message Authentication (DMARC)

Content Body Based Methods

FortiGuard Spam Checksum DB

Advanced Newsletter and Suspicious Newsletter Detection

Attachment/Content Filtering	Third Party SPAM URI real-time blocklists (SURBL)
Extensive Dynamic Heuristic spam filters	Behavioral analysis
Bayesian Statistical Filtering	Image analysis scanning
Anti-Malware Detection	PDF analysis scanning
FortiGuard Full Category Web Content Filtering (includes Spam, Phishing and Malware URLs)	Banned word filtering
	Dictionary filtering (HIPAA, SOX, GLB)
FortiGuard Spam Outbreak detection	Domain Keys Identified Mail (DKIM)

FortiMail is designed to perform email threat detection in both inbound and outbound direction

- Inbound threat detection protects users
- Outbound threat detection is critical to protect the reputation of the network and domain

What malware protection methods are available?

This question is commonly posed during tenders where the need multiple AV engines are stipulated as mandatory. Fortinet uses multiple layers of malware detection and threat neutralization technology to achieve email security:

FortiGuard Antivirus - FortiGuard Antivirus protects against the latest viruses, spyware, and other content-level threats. It uses industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and accessing its invaluable content.

FortiGuard Virus Outbreak - FortiGuard Virus Outbreak is a file hash reputation based service using multiple sources of outbreak information to identify emerging threats. Sources include both Fortinet and Third Party Threat Sources:

- FortiGuard pre-signature hashes
- FortiSandbox Global Threat Network Hashes
- Cyber Threat Alliance Sources

FortiGuard Malware Outbreak - FortiGuard sees millions of queries per minute on emails and attachments; good and bad, known and unknown across the globe. Fortinet perform metadata analysis on these queries to identify new threats and prevent new outbreaks.

FortiSandbox - FortiSandbox is a core part of the Fortinet Advanced Threat Protection (ATP) solution integrating with FortiMail as part of the Fortinet Security Fabric . FortiSandbox delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and mitigation.

Threat Neutralization - Removal of all potentially malicious content from emails and archive of original content.

Content Disarm and Neutralization
*** Supported in FortiMail 5.4.2** - FortiMail supports* the removal of active content including macros, activescript, URLs, links etc. from Word and PDF files and reconstruction in a clean, neutralized file format.

Why FortiGuard Virus Outbreak and FortiGuard Malware Outbreak. It is confusing?

We agree, but it was necessary to avoid disruption to existing customers. FortiGuard Malware Outbreak came first and as it was based on queries to the FortiGuard AntiSpam DB and required this license to function. When we launched the new Virus Outbreak service, this was a new feature and a new license created for it. Over time this license will include new features including Content Disarm and Neutralization and eventually Malware Outbreak will be rolled into this license. Rather than take a useful feature away, it was decided to keep the features separate to allow the new Virus Outbreak license to be more widely adopted and even included in the bundle before changing licensing.

How is FortiMail Managed?

FortiMail is managed via a modern HTML5/JS based GUI or via the CLI (SSH, Telnet or Console). A REST API is also available for programmatic control or integration with provisioning systems.

Will compressed email attachments be scanned and can FortiMail reject attachments based on policies defined and attachment type?

Yes. The FortiMail antivirus system is based on the same award winning ICSA Labs and VB100 certified technology that is used in Fortinet's FortiClient PC software. Compressed attachments and nested archives are scanned for malicious content to ensure proper email hygiene whilst protecting comprehensively against compression attacks (zip bomb).

Does FortiMail Support Secure Email Delivery?

FortiMail provides TLS and S/MIME encryption for secure email transmission as well Identity Based Encryption (IBE) which allows users to send email securely to someone without any pre-existing relationship, PKI, key exchange, or client software. Literally anyone with a web browser and an email account can receive encrypted email from a FortiMail,

What are the benefits of IBE?

IBE offers organizations a simple, effective, affordable way to encrypt messages. There is no additional hardware or software to install or users to provision. The recipient does not have to generate key pairs in order to read the encrypted document.

Unlike traditional public-key cryptography that relies on specialized hardware or clients, IBE makes it very easy for organizations to send encrypted communication to users, and for those users to read encrypted emails. Organizations can choose either push (delivering the email to the user) or pull methods (sending the user a notification of mail waiting for them on the FortiMail server) of delivering encrypted content. Organizations can also use a combination of methods (such as push for all messages less than 1 MB in size, and pull for all messages over 1 MB).

Any organization that is looking to reduce the cost of paper-based communications that contain confidential or regulated data, such as financial statements, health care communications, and legal documents, can benefit from FortiMail IBE. They can replace their paper-based communications with secure email, eliminating the per-letter cost and environmental impact of mailing letters.

How Does IBE work?

When an outbound email arrives at the FortiMail unit, it applies predefined policies to determine if the message requires encrypting (for example, based on keywords in the message body or header, or recipient domain). If the email requires encryption because of a policy match, the FortiMail unit encrypts the message using the public key.

Pull Method (encrypted email is stored on the FortiMail device)

1. The FortiMail device sends the recipient an email to notify that a new encrypted message is available.
2. Recipient clicks on the link in the notification, which creates a browser-based SSL connection with the originating FortiMail device.
3. The recipient authenticates with FortiMail (typically the recipient will authenticate via LDAP). The first time user will have to register to create an account on the local FortiMail device.
4. The FortiMail device issues the private key to decrypt the email and the user opens the encrypted email.

Push Method (encrypted email is sent to the user)

1. The FortiMail device sends the recipient the encrypted message.
2. Recipient clicks on the html attachment to the encrypted message, which creates a browser-based SSL connection with the originating FortiMail device.
3. The recipient's mail client posts the encrypted data to FortiMail's web server for decryption.
4. The recipient authenticates with the FortiMail device (a first-time user will have to register to create an account).
5. The FortiMail device issues the private key to decrypt the email and the user opens the encrypted email

Can the FortiMail units be used to support many email domains?

Yes. FortiMail support multiple email domains. This allows companies and service providers to support secure multitenant email deployments using a shared FortiMail platform. See the datasheet for details of how many domains are supported for each model.

What type of email DoS security is available in the FortiMail security platform?

FortiMail offers several key Denial-of-Service features to secure against email related DoS attacks: Mail Bombing Attacks, Recipient Address Attacks, Email Flooding Attacks, and Mail Spoofing. In addition FortiMail offers user configurable rate limiting options and sender reputation to combat email DoS attacks.

What types of email quarantine options are available?

FortiMail offers both system level and user configurable options to quarantine emails infected with viruses and emails identified as spam. In addition the FortiMail offers email user notification of tagged emails and options to recover or delete emails tagged as spam.

What types of email archiving options are available?

FortiMail offers local as well as external email archiving options to meet government and regulatory compliance for standards such as Sarbanes Oxley. FortiMail offers user configurable and granular policy controls including archiving options based on key words, specific domains and users, or dictionary content.

What logging and reporting features do the FortiMail systems offer?

FortiMail offers extensive and granular logging and reporting features to give mail administrators complete visibility into their organizations email activity. Logging can be used to track all emails entering and leaving your email servers. FortiMail reporting provides granular email auditing features such as on-demand and schedules reports with hundreds of options to generate reports based on sender, recipient, domain, day, week, month, spam and virus activity and many other options.

As well as on-box reporting, FortiMail supports logging to a central FortiAnalyzer for log aggregation and reporting.

What types of user authentication methods are available?

In gateway and transparent mode, FortiMail supports user authentication to external servers, including RADIUS, LDAP, SMTP, IMAP, and POP3 servers. In addition specific email routing is supported by recognition of LDAP attributes.

Login to the Webmail interface (server mode) or Quarantine interface (all modes) supports the use of Single Sign-on acting as a SAML 2.0 SP to a third party IdP.

How is the FortiMail system managed?

FortiMail system administration can be performed via most modern web browsers supporting JavaScript such as Chrome, IE/Edge, Firefox, etc, as well as via the CLI using SSH or Telnet. End users can access quarantined email and edit user preferences, such as personal white/black lists using any JavaScript enabled web browser. In gateway and transparent mode, end user can access quarantined emails through POP3 and secure POP3S. When in server mode, end users can access their mailboxes via POP3/POP3S and IMAP/IMAPS.

Why should I buy a FortiMail instead of a FortiGate with antispam features?

FortiMail is Fortinet's premier antispam service platform. It supports over sixteen different spam detection methods including Outbreak Protection, Behavioral Analysis , greylisting, and image analysis features that are not available on the FortiGate platform. It also supports full Mail Transfer Agent (MTA) features and can perform user-based antispam rules. If you want the highest possible accuracy and control in detecting spam then you want a FortiMail system.

Can I protect my users from offensive content?

FortiMail has multiple methods to prevent users sending or receiving such content including:

- Built in profanity dictionary
- URL filter to filter emails linking to offensive content
- Dynamic Adult Image Analysis to identify emails containing adult images

Which standards does FortiMail support?

FortiMail supports the expected SMTP standards including but not limited to RFC 5321, RFC 3207, RFC 3463. FortiMail also implements internet standards such as Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-Based Message Authentication (DMARC).

For an exhaustive list of Supported RFCs see Appendix A of the FortiMail Administration Guide.

Deployment FAQs

What deployment options are supported?

FortiMail can be deployed in on-prem hardware, virtual machine, public cloud appliance formats and as a managed service (this is covered separately in the FortiMail Cloud FAQ). FortiMail appliances can be deployed in gateway, inline and server modes – an unparalleled flexibility which makes FortiMail the ideal solution for any email security requirement.

Which mail servers are supported?

FortiMail is compliant with SMTP RFCs and therefore supports any equivalently compliant mail server solutions including, but not limited to Microsoft Exchange, Office365, Exchange On-line, Gmail, IBM Lotus Domino, Sendmail, Novell Groupwise etc.

Does FortiMail support redundancy or high availability?

Yes, FortiMail supports a high availability configuration that offers full synchronization of configuration and mail data between two FortiMail systems to ensure maximum availability of email services. See the FortiMail Administration Manual for more information.

How can I scale my solution?

FortiMail supports active-active high availability which delivers linear scalability and differing models can be utilized in a cluster allowing customers to maximize the ROI.

Do I need a FortiSandbox?

FortiSandbox is not a pre-requisite to run a FortiMail, but it does have significant benefit in Advanced Threat Protection (ATP) and both are tightly integrated key parts of the Fortinet Security Fabric integration.

On-prem FortiSandbox Appliance vs FortiSandbox Cloud?

Whether to choose an on prem solution vs FortiSandbox Cloud depends on many factors such as privacy concerns with processing files outside of the organization, ability to guarantee and scale sandbox resource, ability to run custom “Gold” VM images, ability to control and run multiple OS versions etc. To understand which solution is most suitable for an organization, please engage your Regions FortiMail CSE.

Why would I choose FortiMail Appliance vs FortiMail Cloud Managed Service?

The FortiMail Cloud Managed service is based on the same FortiMail solution as the appliances, the difference being that it is offered as a managed service, operated by Fortinet. Which option you choose depends on factors such as an organizations appetite to outsource to the cloud, internal IT resource, need to avoid capital expenditure, organizational growth and need for predictable per headcount costs etc.

Subscription Service Questions

Are automatic antivirus and antispyware updates available from Fortinet’s FortiGuard Network?

Yes. All antivirus signatures, scanning engine updates, heuristics signatures and other related functions are fully supported by Fortinet’s FortiGuard Distributed Network (FDN) to provide real-time proactive updating of the FortiMail systems. This ensures that the latest virus signatures are always available to protect corporate users from the latest email threats.

How is the antispam database updated?

There are many different antispam features offered. Some are dynamic, such as the FortiGuard Antispam service and some are configured by the administrator with Bayesian filters or a banned word blocklist. You can use these various features in any combination based on configurable policies. Only the FortiGuard Antispam service is a subscription based service where both email headers and email content is verified against a dynamically maintained database for up to the minute accuracy with the latest known spammers.

What is the subscription/licensing scheme for the FortiMail and FortiGuard Services?

Like all Fortinet devices, FortiMail is licensed on a per unit basis, which means that you can have any many users as the FortiMail unit can handle. There are no per user licenses like other popular mail protection solutions that can increase costs significantly as the company grows. This makes the FortiMail platform extremely cost effective and helps lower Total Cost of Ownership (TCO) and provides rapid Return-on-Investment (ROI). There are currently 5 subscription licenses for FortiMail:

FortiGuard AV Services	-	Antivirus subscription
FortiGuard AS Service	-	Anti-Spam subscription
FortiCloud Sandbox Service	-	Cloud based sandboxing service for files and URLs
FortiGuard Virus Outbreak Protection Service	-	New Virus Outbreak service protecting against emerging threats.
Dynamic Adult Image Analysis Service	-	Real-time image analysis to detect adult image content in emails

What is included in the bundles?

FortiMail bundles currently include the FortiGuard AV Services and AS Service, together with a FortiCare Support Contract. This may be changed in the future to include the other subscriptions.

Which subscription is required for each feature?

Malware

Feature:	Licensed by:	Effect when license expires:
FortiGuard AV	FortiGuard AV Service	AV continues to function but engine/signatures do not update. Over time, AV will become out of date.
Virus outbreak	FortiGuard Virus Outbreak Protection Service	Requires license to function
Grayware	FortiGuard AV Service	Requires license to function
AV Heuristic	FortiGuard AV Service	Requires license to function
File signature check	Not licensed	Not licensed, continues to function without licenses
FortiSandbox (On-Prem)	Not licensed	No license required (requires on-prem FortiSandbox)
FortiSandbox (Cloud)	FortiCloud Sandbox Service	Requires license to function

Anti-Spam

FortiGuard IP Reputation	FortiGuard AS Service	Requires license to function
FortiGuard URI Filtering	FortiGuard AS Service	Requires license to function
FortiGuard Spam Outbreak Protection	FortiGuard AS Service	Requires license to function
Greylist	Not licensed	Functions fully
SPF Check	Not licensed	Functions fully
DMARC check	Not licensed	Functions fully
Behavior analysis	FortiGuard AS Service	Requires license to function
Header analysis	FortiGuard AS Service	Requires license to function
Heuristic	FortiGuard AS Service	Will function, however heuristics database will not update
SURBL	Not licensed	Functions fully
DNSBL	Not licensed	Functions fully
Banned Word	Not licensed	Functions fully
Safelist Word	Not licensed	Functions fully
Dictionary	Not licensed	Functions fully

Image spam	Not licensed	Functions fully
Bayesian	Not licensed	Functions fully
Suspicious newsletter	FortiGuard AS Service	Requires license to function
Newsletter	FortiGuard AS Service	Requires license to function

Content

Dynamic Adult Image Analysis	Dynamic Adult Image Analysis Service	Requires license to function
Content Disarm and Reconstruction	FortiGuard Virus Outbreak Protection Service	Requires license to function

What happens when a license expires?

In all cases, when a license expires, email will continue to flow unhindered, however the catch rate may decrease. Users can continue to send and receive mail and have full access to the quarantine.

When the FortiCloud Sandbox Service expires, the submission limits will revert back to the free submission limits where the FortiMail device can submit 100 files per day.

What happens when a VM Trial license expires?

When a VM license expires, usually all the subscription licenses will expire at the same time, reducing the security protection provided by the FortiMail. Access to the GUI will also be restricted to the Dashboard and basic system administration features only to allow basic management of the device and addition of a new license. Users will no longer be able to access the user quarantine.

Appliance FAQs

I need redundant PSU, which model do I need?

Redundant PSU is supported out of the box on the FML1000D upwards. A redunedn PSU can be ordered from the accessories tab of the pricelist and fitted to the FortiMail 400E.

Is Fortimail available in a Virtual Machine format?

FortiMail is compatible with VMWare ESXi, Hyper-V, Citrix XenServer and KVM/QEmu. FortiMail-VM is licensed based on the vCPU count with 1, 2, 4 and 8, 16 and 32 vCPU options.

Compliance FAQs

Which FortiMail products are RoHS (Removal of Hazardous Substances) compliant?

All FortiMail models shipping today RoHS compliant.

Where is FortiMail manufactured?

FortiMail appliances are manufactured in the US with all development being performed in Canada.

What standards does FortiMail hold?

FortiMail is FIPS 140-2 and Common Criteria EAL2+ (4.2.2) and NDPP (5.2.6) certified.

I need a G/USG SKU but do not see them. Can you create them?

G and USG SKUs are often requested for deployment in US federal deployments but are not generally required.

G SKUs - Specifies the device was manufactured in the US

USG SKUs - Specifies the device was manufactured in the US and has special firmware installed which only

communicates with US servers

As all FortiMail devices are manufactured in the US, there is no need for a specific G-SKU. If confirmation is required, a letter can be provided to this extent. USG-SKUs and the specialized firmware has never been needed for any federal deal in the US. Setting of the firmware to communicate only with US network is possible in the standard firmware.

If there is an insistence that USG firmware is necessary, this can be achieved but:

- This will require at least 3 months development effort
- USG SKUs would be limited to high end models only
- There will be a minimum order quantity commitment needed
- All SKUs will incur a 20% uplift due to the additional effort

Is FortiMail compliant with US DHS - Binding Operational Directive 18-01?

In short – yes.

This directive, detailed here https://cyber.dhs.gov/ specifies several requirements for email systems (summarized for brevity):

Within 90 days of issuance of the directive (by January 15, 2018):

- Configure all internet-facing mail servers to offer STARTTLS.
  Enabled through the setting System > Mail Settings > Mail Server Setting > SMTP over SSL/TLS
- Configure all second-level domains to have valid SPF/DMARC records, with at minimum a DMARC policy of "p=none" and at least one address defined as a recipient of aggregate and/or failure reports.
  This is an external requirement for this to be configured in DNS and has no impact on FortiMail.

Within 120 days of issuance of the directive (by February 13, 2018):

- Disable SSLv2 and SSLv3 on web and mail servers.
  Supported via CLI configuration:

```
config system global
   set ssl-versions tls1_1 tls1_2
end
```

- Disable 3DES and RC4 ciphers on web and mail servers.
  Supported via CLI configuration:

```
config system global
set strong-crypto enable
end
```